IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION

DHI GROUP, INC., F/K/A DICE HOLDINGS, INC. AND RIGZONE.COM, INC.,	§	
	§	
Plaintiffs,	§	
	§	
v.	§	CIVIL ACTION NO. H-16-1670
	§	
DAVID W. KENT, JR. SINGLE INTEGRATED OPERATIONS PORTAL, INC. D/B/A OILPRO AND OILPRO.COM, ESTEVAN DUFRIN, MATTHEW KENT, BRYAN ROBINS, JEREMY ANTONINI, AND JOHN DOE NOS. 1-10,	§	
	§	
	§	
	§	
	§	
	§	
Defendants.	§	

<u>**MEMORANDUM AND RECOMMENDATION**</u>

Pending before the court[1] is Defendant Jeremy Antonini's ("Antonini") Motion to Dismiss (Doc. 77). The court has considered the motion, Plaintiffs DHI Group, Inc., f/k/a Dice Holdings, Inc. ("DHI") and Rigzone.com's ("Rigzone") (collectively, "Plaintiffs") response (Doc. 86), Antonini's reply (Doc. 87), all other relevant filings, and the applicable law. For the reasons set forth below, the court **RECOMMENDS** that Antonini's motion to dismiss be **GRANTED IN PART** and **DENIED IN PART**.

I. Case Background

Plaintiffs filed a complaint on June 10, 2016, alleging

---

[1]   This case was referred to the undersigned magistrate judge pursuant to 28 U.S.C. § 636(b)(1)(A) and (B), the Cost and Delay Reduction Plan under the Civil Justice Reform Act, and Federal Rule of Civil Procedure 72. <u>See</u> Doc. 4, Ord. Dated June 16, 2016.

violations of the Computer Fraud and Abuse Act ("CFAA"), the Stored Wire and Electronic Communications and Transactional Records Access Act ("SCA"), the Racketeer Influenced and Corrupt Organizations Act ("RICO"), the Texas Uniform Trade Secrets Act ("TUTSA"), the Texas Harmful Access by Computer Act ("THACA"), the Texas Theft Liability Act ("TTLA"), as well as claims for misappropriation of confidential information, conversion, trespass to chattels, fraud, breach of fiduciary duty, unfair competition, tortious interference with present and prospective business relationships, civil conspiracy, and aiding and abetting.[2]

A.   Factual Background

The following factual account is derived from Plaintiffs' live complaint.

1.   The Creation of Rigzone

Defendant David Kent created a website called Oceandril Data Services in 2000 where users could offer oil and gas equipment for sale.[3]   The name of the website was later changed Rigzone.com and it began offering other services, including job postings for the oil and gas industry in the Houston and Gulf Coast Region.[4]

DHI purchased Rigzone for fifty-one million dollars in August 2010; David Kent received approximately thirty-five million dollars

---

[2]   See Doc. 1, Pls.' Compl.

[3]   See id. p. 6.

[4]   See id.

from the sale due to his seventy-percent ownership stake.[5] The sale included Rigzone's website and assets.[6] Other defendants, including Matthew Kent, Bryan Robins, and Antonini also received a portion of the sale proceeds and continued to work for Rigzone after the sale.[7] DHI later acquired two other job posting websites, World Wide Worker and Oil Careers, in an effort to provide a single platform for professionals in the energy industry under the name Rigzone.[8]

Members of Rigzone were given a username and password, and after logging in, they could create a profile, upload their resume, and apply for jobs.[9] Once a member uploaded a resume, it was given a unique number, and each profile was stored in Rigzone's member database.[10] Recruiters and employers would pay Rigzone to have direct access to Rigzone members about job opportunities.[11] Only those who paid to use Rigzone's database had access to it.[12] Rigzone also generated revenue by selling advertisement space on

---

[5] See id.

[6] See id. pp. 6-7.

[7] See id. p. 7.

[8] See id.

[9] See id. p. 8.

[10] See id.

[11] See id.

[12] See id.

its website.[13]   In order to safeguard the information contained in
its member database, Rigzone invested in a variety of security
measures, including password protection for employee computers and
the hiring of computer specialists to update its security measures
regularly.[14]   Former employees of Rigzone were not permitted to
access Rigzone's internal computer system.[15]

2.   Sale of Rigzone and Launch of Oilpro

In January 2012, David Kent's consulting agreement expired,
and he created Single Integrated Operations Portal, Inc.
("SIOPCO"), which became Oilpro's parent company.[16]   After the
expiration of his non-compete clause, David Kent publicly launched
Oilpro on October 1, 2013.[17]

Oilpro was able to start up with a large membership base
because David Kent accessed, without permission, Rigzone's computer
system, including its member database, after he sold it to DHI.[18]
This software backdoor to Rigzone's computer system allowed David
Kent to view the private resumes on Rigzone's site without its

---

[13]   See id.

[14]   See id. p. 9.

[15]   See id.

[16]   See id. p. 11.

[17]   See id. p. 9.

[18]   See id. pp. 9-10.

knowledge.[19] Additionally, David Kent persuaded a Rigzone employee
to make a backup copy of Rigzone's database and instructed another
employee to download a backup copy to an external hard drive.[20]
These copies disappeared after David Kent left Rigzone.[21]

Rigzone soon began losing employees to Oilpro.[22]   Estevan
Dufrin ("Dufrin") began working for Oilpro in December 2013, one
month after he left Rigzone's employment.[23] Matthew Kent, David
Kent's brother and a former vice president of sales for Rigzone
before and after it was acquired by DHI, was also hired by Oilpro.[24]
As vice president of sales, Plaintiffs allege that Matthew Kent was
familiar the inner workings of the Rigzone member database, the
details of Rigzone's relationships with employers and recruiters,
and the methodology that Rigzone used to grow its membership.[25]

Robins worked for Rigzone as a vice president of sales, prior
and subsequent to its acquisition by DHI.[26] He was later hired by
Oilpro as head of advertising sales.[27] Plaintiffs allege that based

---

[19]   See id. p. 10.

[20]   See id. p. 11.

[21]   Id.

[22]   Id. pp. 11-13.

[23]   See id. p. 11.

[24]   See id. p. 12.

[25]   See id.

[26]   See id.

[27]   See id.

on Robins' employment at Rigzone, he understood the methodology of Rigzone's advertising sales and would have known that the swift membership growth of Oilpro was unrealistic and was not acquired by legitimate means.[28] Robins "had the experience, skills, position, opportunity, and motive to support, assist, and participate with David Kent, Oilpro, and others in the illegal and tortious conduct" and he "worked closely with David Kent" at Oilpro.[29]

Antonini became chief of technology for Oilpro after leaving Rigzone, where he had served as vice president of technology prior and subsequent to DHI's acquisition of Rigzone.[30] Antonini was well versed in Rigzone's technology and, along with David Kent, was the "most familiar with the code for Rigzone."[31] Antonini "worked closely with David Kent and had the experience, skills, position, opportunity, and motive to support, assist, and participate with David Kent, Oilpro, and others in the illegal and tortious conduct towards the Plaintiffs."[32]

The former employees from Rigzone, including Antonini, Robins, Dufrin, and Matthew Kent, became partial owners of Oilpro.[33] Aside from David Kent, the employees of Oilpro owned around fifteen

---

[28]   See id.

[29]   See id. pp. 12-13.

[30]   See id. p. 13.

[31]   Id.

[32]   Id.

[33]   See id.

percent of the company.[34]

3. Hacking of Plaintiffs' Information

Several different rounds of hacks took place from late 2013 through 2016.

a. First Round of Hacks

David Kent accessed Rigzone's member database on February 6, 2014.[35] Rigzone learned of potential hacking on February 26, 2014, when one of Rigzone's members told Rigzone's customer service that she had received an email solicitation from Oilpro.[36] Rigzone conducted a review that showed that no Oilpro employee accessed the profile through an authorized account.[37]

As a result of this hacking, two DHI employees created fake accounts with information only accessible through Rigzone's member database to track potential future hacking.[38] These two fake members received email solicitations on April 14, 2014, from Oilpro asking them to create Oilpro profiles.[39] Rigzone determined that no Oilpro employee viewed these profiles by using Rigzone's website and no Rigzone user had looked at both profiles.[40] On April 14,

---

[34]   See id.

[35]   See id. p. 15.

[36]   See id.

[37]   See id.

[38]   See id.

[39]   See id.

[40]   See id.

2014, other Rigzone members received email solicitations from Oilpro to become members.[41] Oilpro obtained these email addresses by accessing 13,000 profiles in Rigzone's member database between April 4, 2014, and April 6, 2014.[42]

Rigzone checked its computer systems and determined that from October 17, 2013, through April 15, 2014, 100,000 suspect hypertext transport protocol ("HTTP") requests[43] went out to Rigzone's member database through the internet.[44] These HTTP requests sought resumes from the Rigzone member database by "direct[ing] the [database] to give the user access to specific resumes" and were created by capitalizing on Rigzone's unique source code.[45] Only the creators of the source code, including David Kent, knew its particulars.[46] These HTTP requests came frequently and accessed a large volume of resumes, indicating that they were carried out by a computer program, not by manual inputs.[47]

The HTTP requests originated from twenty-three different IP addresses, twenty-two of which were registered to UK Dedicated

---

[41]   See id. p. 18.

[42]   See id.

[43]   "An HTTP request is a computer code command transmitted to a website over the internet." Id.

[44]   See id. pp. 15-16.

[45]   Id. p. 16.

[46]   See id.

[47]   See id.

Servers Limited ("UK DSL"), a company that conceals its customers' IP addresses.[48]   One of David Kent's email addresses maintained an account with UK DSL, and this email address received information from UK DSL near the time of these first hacks.[49]   The other IP address that was not registered with UK DSL was registered to SIOPCO, Oilpro's parent company.[50]   On February 6, 2014, February 7, 2014, April 3, 2014, and April 15, 2014, the dates of the HTTP requests, some of the concealed IP addresses logged into a social media account of David Kent.[51]

These first hacks resulted in access of information from 98,000 resumes of Rigzone members which led to an increase in the use of Oilpro's website, including by Rigzone members whose profiles were hacked by Oilpro.[52]   On April 24, 2014, David Kent reached out to DHI stating that he had received an investment offer and that he built Oilpro with a potential future acquisition by DHI in mind.[53]   DHI declined to buy Oilpro or provide investment funds at that time.[54]

     b.   **Hacks of Google Analytics Data**

---

[48]   See id.

[49]   See id. p. 17.

[50]   See id.

[51]   See id.

[52]   See id.

[53]   See id. p. 18.

[54]   See id.

Google Analytics provides information for websites, "including (1) number of visits to the website, (2) number of new users, (3) pages viewed per visit, and (4) average duration of each visit."[55] Google Analytics users must log into their accounts via a password.[56] Plaintiffs maintained a Google Analytics account protected by a password.[57]

Dufrin, who left Rigzone on November 27, 2013, accessed Plaintiffs' Google Analytics account and sent the information to David Kent.[58] David Kent sent Dufrin an email on January 20, 2015, asking how the Oilpro Google Analytics data compared to their "friend's site."[59] In response, Dufrin accessed Plaintiffs' Google Analytics account and forwarded to David Kent specific private information about Rigzone's website, including page views.[60]

On June 10, 2015, Dufrin sent an email to David Kent stating, "So, I'm trying to scratch the engagement on Rusty[61] a bit and noticed that the folks searching their jobs are 75% return users

---

[55]   Id.

[56]   See id.

[57]   See id.

[58]   See id. pp. 18-19.

[59]   Id. p. 19.

[60]   See id.

[61]   Plaintiffs allege that Rusty was Oilpro's code name for Rigzone, as evidenced by an email sent by David Kent on December 8, 2014, stating "Rusty = [Rigzone]. Much easier to say and conveys [Oilpro] is the new, non-rusty solution to all of your oil & gas data needs. Also protects my feelings because at one point, that was a product I loved . . . it has just gotten a bit rusty." Id. pp. 19-20.

regardless of the source."[62]   David Kent replied with two separate
emails to Dufrin stating that they should have someone "scrape"[63]
full time to equal or surpass the job listings of Rigzone and that
Oilpro should hire someone to post all the "Rusty jobs."[64]

c. Second Round of Hacks

On June 11, 2015, David Kent sent an email to Dufrin regarding
hiring a freelancer "for web scraping/crawling/automated data
extraction solutions," and stated that he wanted to hire the
freelancer to "scrape job boards including resume databases" to
"find backdoors, etc."[65]   Dufrin replied, also hoping that this
potential freelancer could find a "backdoor to full CVs."[66]

On July 20, 2015, an employee of DHI commenced making a
profile on Rigzone, but failed to complete it and it was never
published on Rigzone's member database.[67]   However, this employee
was solicited by Oilpro by email.[68]   Rigzone's computer systems
revealed that from June 17, 2015, to August 2, 2015, 750,000
suspect HTTP requests were sent to the Rigzone member database via

---

[62]   Id.

[63]   "Scraping" "refer[s] to automated programs that extract large amounts
of data from websites. Id. p. 21.

[64]   Id. p. 20.

[65]   Id.

[66]   Id. pp. 20-21.

[67]   See id. p. 21.

[68]   See id.

the internet.[69]   Ten IP addresses, none of which were used in the first hacks, were used for these HTTP requests.[70]   At least two of these IP addresses were registered to UK DSL, and at least one was registered to SIOPCO.[71]   These hacks were different from the first hacks because they targeted Rigzone's resume_writer.asp[72] file.[73] These hacks resulted in the access of information from 700,000 resumes in Rigzone's member database.[74]

On October 25, 2015, David Kent contacted DHI, telling its CEO that Oilpro had acquired an investor.[75]   David Kent also represented that he thought Rigzone would be the best fit for Oilpro's software.[76]   DHI again declined to invest in, or acquire, Oilpro.[77]

d.   Attempted Third Round of Hacks

On October 28, 2015, David Kent again contacted the CEO of DHI to tout Oilpro's success. Kent attributed Oilpro's 540,000 members to what he called "LinkedIn style growth hacks," a software program where members of Oilpro were asked to upload their LinkedIn.com

---

[69]   See id.

[70]   See id.

[71]   See id.

[72]   "A '.asp' page file is script that generates web page content." Id.

[73]   See id. pp. 21-22.

[74]   See id. p. 22.

[75]   See id.

[76]   See id.

[77]   See id.

("LinkedIn") contacts.[78] Once those contacts were uploaded, Oilpro was able to contact these persons with invitations to join the site.[79]

In response to questions from the CEO of DHI, David Kent replied by email one week later, explaining that Oilpro's growth was attributed to its LinkedIn strategy.[80] On November 11, 2015, David Kent sent another email to the CEO of DHI, where he reiterated Oilpro's LinkedIn strategy and mentioned that Oilpro also used traditional marketing approaches for growth.[81] On November 25, 2015, David Kent sent another email to the CEO of the DHI where he discussed Oilpro's investor, a venture capital firm, stating that it had "invested $3,000,000 at a $20,000,000 valuation."[82]

The CFO, CEO, and General Counsel of DHI had a conference call with David Kent on December 8, 2015, about the potential sale of Oilpro to DHI.[83] David Kent stated that Oilpro's top method for growth was their LinkedIn strategy.[84] David Kent "also attributed the growth of Oilpro to 'effort' and the fact that oil and gas is

---

[78]   See id.

[79]   See id. pp. 22-23.

[80]   See id. p. 23.

[81]   See id. pp. 23-24.

[82]   Id. p. 24.

[83]   See id.

[84]   See id.

a 'safe haven industry.'"[85] The CEO of DHI stated that he would be interested in further discussions about an acquisition or merger, and David Kent reiterated that he wanted to work with DHI more than any other investor.[86]

On December 11, 2015, five suspect HTTP requests came to Rigzone's member database seeking resume information.[87] However, Rigzone had changed the resume.asp file, so no resumes were taken from the database.[88] One of the IP addresses used for the suspect HTTP request was registered to David Kent's UK DSL account.[89] This account was accessed by an IP address associated with SIOPCO around the time of the attempted third hack.[90] On December 13, 2015, an IP address from David Kent's home in Spring, Texas, accessed the UK DSL account.[91]

David Kent met with DHI in New York City on January 20, 2016.[92] David Kent again emphasized Oilpro's LinkedIn growth strategy, expressing "that this 'network effects' strategy was the 'core way' and 'enough' to grow Oilpro to over 500,000 members in a short

---

[85]   Id.

[86]   See id.

[87]   See id. p. 25.

[88]   See id.

[89]   See id.

[90]   See id.

[91]   See id.

[92]   See id.

period of time."[93]

After this meeting, David Kent sent the CEO of DHI a spreadsheet containing Oilpro's membership growth figures.[94] Oilpro acquired 3,085 new members in December 2013, 4,486 in January 2014, 12,131 in February 2014, 28,763 in April 2014, 45,936 in June 2014, and 45,823 in September 2015.[95] By January 2016, Oilpro grew to at least 500,000 members.[96]

Overall, around 796,000 Rigzone accounts containing 586,560 email addresses were hacked by Oilpro, and Oilpro sent 17.7% of these email addresses invitations to join Oilpro.[97] As a result, 111,000 of the hacked accounts ended up joining Oilpro.[98]

4.   Criminal Complaint

On March 23, 2016, the Federal Bureau of Investigation filed a criminal complaint against David Kent, alleging violations of 18 U.S.C. §§ 371, 1343, and 2.[99] David Kent was charged with conspiracy to violate 18 U.S.C. §§ 1030(a)(2)(C), 1030(c)(2)(B), and 1343, and wire fraud and aiding and abetting wire fraud under

---

[93]   Id. p. 26.

[94]   See id.

[95]   See id. pp. 26-27.

[96]   See id. p. 14.

[97]   See id. pp. 17-18.

[98]   See id. p. 18.

[99]   See id. p. 29.

18 U.S.C. §§ 1343 and 2.[100]   A criminal information was filed
against David Kent on June 3, 2016, in the U.S. District Court for
the Southern District of New York, alleging conspiracy and wire
fraud.[101]

B.   **Procedural Background**

Plaintiffs filed their complaint on June 10, 2016, alleging
claims of civil conspiracy and aiding and abetting against
Antonini.[102]   Antonini filed the pending motion to dismiss on
December 30, 2016, arguing that Plaintiffs failed to state a claim
against him and venue was improper.[103]   Plaintiffs responded on
January 20, 2017, and Antonini replied on January 27, 2017.[104]

II.   **Legal Standard**

Pursuant to Federal Rule of Civil Procedure ("Rule") 12(b)(6),
dismissal of an action is appropriate whenever the complaint, on
its face, fails to state a claim upon which relief can be granted.
When considering a motion to dismiss, the court should construe the
allegations in the complaint favorably to the pleader and accept as
true all well-pleaded facts.   Sullivan v. Leor Energy, LLC, 600
F.3d 542, 546 (5th Cir. 2010).

---

[100]   See id.

[101]   See id.

[102]   See Doc. 1, Pls.' Compl.

[103]   See Doc. 77, Antonini's Mot. to Dismiss.

[104]   See Doc. 86, Pls.' Resp. to Antonini's Mot. to Dismiss ["Pls.'
Resp."]; Doc. 87, Antonini's Reply to Pls.' Resp. to Antonini's Mot. to Dismiss
["Antonini's Reply"].

A complaint need not contain "detailed factual allegations" but must include sufficient facts to indicate the plausibility of the claims asserted, raising the "right to relief above the speculative level." Bell Atl. Corp. v. Twombly, 550 U.S. 544, 555 (2007); see also Ashcroft v. Iqbal, 556 U.S. 662, 678 (2009). Plausibility means that the factual content "allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." Iqbal, 556 U.S. at 678. A plaintiff must provide "more than labels and conclusions" or "a formulaic recitation of the elements of a cause of action." Twombly, 550 U.S. at 555. In other words, the factual allegations must allow for an inference of "more than a sheer possibility that a defendant has acted unlawfully." Iqbal, 556 U.S. at 678.

Rule 8(a)(2) requires only "a short and plain statement of the claim showing that the pleader is entitled to relief," in order to "give the defendant fair notice of what the . . . claim is and the grounds upon which it rests." Twombly, 550 U.S. at 555. When a plaintiff's complaint fails to state a claim, the court should generally give the plaintiff at least one chance to amend under Rule 15(a) before dismissing the action with prejudice. See Great Plains Trust Co. v. Morgan Stanley Dean Witter & Co., 313 F.3d 305, 329 (5th Cir. 2002) ("[D]istrict courts often afford plaintiffs at least one opportunity to cure pleading deficiencies before dismissing a case, unless it is clear that the defects are

incurable or the plaintiffs advise the court that they are unwilling or unable to amend in a manner that will avoid dismissal."); see also United States ex rel. Adrian v. Regents of the Univ. of Cal., 363 F.3d 398, 403 (5th Cir. 2004) ("Leave to amend should be freely given, and outright refusal to grant leave to amend without a justification . . . is considered an abuse of discretion." (internal citation omitted)).

III. Analysis

Antonini argues that venue is improper in this case, and, alternatively, that certain claims against him should be dismissed. Antonini moves to dismiss Plaintiffs' claims that he aided and abetted in the following common-law causes of action: misappropriation of confidential information, conversion, trespass to chattels, unfair competition, and tortious interference with business relationships. Additionally, Antonini challenges Plaintiffs' claims that he conspired to violate the CFAA, SCA, TUTSA, THACA, and TTLA. The court will address each of Antonini's challenges to these claims.

A. Rule 12(b)(3): Venue

Antonini contends that venue in this case is improper because he lived in the Western District of Texas and worked from home while the events alleged in the complaint took place. Plaintiffs argue that his motion is too late, and that, regardless of the timing, venue in the Southern District of Texas is proper because

it is where a majority of the alleged events took place.

Under 12(b)(3), a defendant may move to dismiss an action for improper venue. Williamson-Dickie Mfg. Co. v. M/V Heinrich J., 762 F. Supp.2d 1023, 1026 (S.D. Tex. 2011)(citations omitted). "The majority of courts conform to the standard that once a defendant has raised the improper venue issue by motion, the burden of sustaining venue rests with the plaintiff." Id. (citing McCaskey v. Cont'l Airlines, Inc., 133 F. Supp.2d 514, 523 (S.D. Tex. 2001); Bigham v. Envirocare of Utah, Inc., 123 F. Supp.2d 1046, 1048 (S.D. Tex. 2000).

Under 28 U.S.C. § 1391, venue is proper in "a judicial district in which any defendant resides, if all defendants are residents of the State in which the district is located" or "a judicial district in which a substantial part of the events or omissions giving rise to the claim occurred." 28 U.S.C. § 1391(b)(1) & (2).

Regardless of whether Antonini's motion was timely, the court finds that venue is proper here. Plaintiffs have alleged that Dufrin and Robins are residents of Harris County, Texas; Antonini was a resident of Bexar County, Texas, but he stated in his reply that he is now a resident of the Northern District of Texas; Matthew Kent is a resident of Coryell County, Texas; David Kent is a resident of Montgomery County; and that Oilpro is a Texas corporation with its principal place of business in Houston, Harris

County, Texas.   Here, all the defendants reside in Texas, and

therefore, the venue may be a judicial district in which any

defendant resides.   Dufrin, Robins, and Oilpro are residents of

Harris County.   Additionally, as Oilpro's principal place of

business is in Houston, Texas, the court finds that this is a

judicial district where a substantial part of the events or

omissions giving rise to the claim occurred.   Therefore, this court

is the proper venue for this action.

B.   Timeliness of the Rule 12(b)(6) Motion

In their response, Plaintiffs contend that Antonini's Rule

12(b)(6) motion is untimely and should be denied.

A Rule 12(b)(6) motion "must be made before the service of a

responsive pleading," but courts, while finding that a post-answer

Rule 12(b)(6) is technically untimely, "do not mechanically or

routinely deny any motion made after a responsive pleading as

untimely."   Puckett v. U.S., 82 F. Supp.2d 660, 663 (S.D. Tex.

1999).   Additionally, Rule 12(h)(2) allows for the defense of

failure to state a claim to be raised later in the case, as a

motion under Rule 12(c) or at trial.   Fed. R. Civ. Pro. 12(h)(2);

Puckett, 82 F. Supp.2d at 663 (citing 5A Charles Alan Wright &

Arthur Miller, Federal Practice and Procedure § 1357 (1990)).

Therefore, courts find if the defendant gave notice by including

these defenses in its answer, then "courts generally allow Rule

12(b)(6) motions filed after the answer . . . but [consider it] a

Rule 12(c) motion for judgment on the pleadings." Puckett, 82 F.

Supp.2d at 663 (citing Delta Truck & Tractor, Inc. v. Navistar

Int'l Transp. Corp., 833 F. Supp. 587, 588 (W.D. La. 1993) (citing

5A Charles Alan Wright & Arthur Miller, Federal Practice and

Procedure § 1357 (1990))). The same standard is applied as in a

Rule 12(b)(6) motion. Puckett, 82 F. Supp.2d at 663 (citations

omitted). Therefore, the court will apply the 12(b)(6) standard to

this motion to determine if Plaintiffs' claims against Antonini

should be dismissed.

C. Aiding and Abetting

Antonini challenges Plaintiffs' aiding and abetting claims,

stating that it is not a recognized cause of action.

1. RICO

In his motion to dismiss, Antonini argues that claims that he

aided and abetted to conspire to violate RICO should be dismissed.

However, in Plaintiffs' response, Plaintiffs state that they "did

not intend to bring an aiding and abetting claim based on RICO,"

and that they adequately pled a RICO claim against some of the

other defendants. Here, as in the case of the motion to dismiss

against Robins, the court finds that Plaintiffs did not plead a

claim of aiding and abetting or conspiracy to violate the RICO

statute against Antonini, and therefore, while there may be RICO

claims against other defendants, there is no RICO claim against

Antonini for the court to dismiss.

2.   State Law Claims

Antonini argues that Plaintiffs' claims of aiding and abetting the following state law claims of: misappropriation of confidential information, conversion, trespass to chattels, unfair competition, and tortious interference with business relationships should be dismissed because Texas law has not recognized aiding and abetting claims for competition-related torts. In the alternative, Antonini contends that the statutes of limitations on these claims have expired. Plaintiffs argue that Texas law has recognized aiding and abetting liability.

Plaintiffs seek to extend aiding and abetting liability to the competition- and theft-related torts of misappropriation of confidential information, conversion, trespass to chattels, unfair competition, and tortious interference with business relationships. In support of this argument, Plaintiffs state that the Texas Supreme Court has recognized claims for aiding and abetting liability, citing cases such as Floyd v. Hefner, 556 F. Supp.2d 617, 654-55 (S.D. Tex. 2008), or Kinzbach Tool Co. v. Corbett-Wallace Corp., 160 S.W.2d 509, 514 (Tex. 1942), in which the court held that Texas law recognized a cause of action for aiding and abetting the breach of a fiduciary duty. Plaintiffs also cite Joe N. Pratt Ins. v. Doane, No. V-7-07, 2008 WL 819011, at *10 (S.D. Tex. Mar. 20, 2008) and In re Am. Airlines, 370 F. Supp.2d 552, 557 n. 10 (N.D. Tex. 2005), which do not address the validity of aiding

and abetting claims under Texas law. See DHI Grp., Inc. v. Kent,

No. 16-1670, 2017 WL 1088352, at *7 (S.D. Tex. Mar. 3, 2017).

In Juhl v. Airington, 936 S.W.2d 640, 643-45 (Tex. 1996), the

Texas Supreme Court discussed "concert of action" liability under

Restatement (Second) of Torts § 876, but declined to apply that

theory of liability. The court cautioned that "[t]he purpose of

the concert of action theory is to deter antisocial or dangerous

behavior," cited cases where courts in other states applied aiding

and abetting liability, and stated that the imposition of liability

occurred in cases that "almost always involved conduct posing a

high degree of risk to others," such as drag racing on public

roads. Id. at 644-45.

In N.Y. Pizzeria, Inc. v. Syal, 56 F. Supp.3d 875, 883-84

(S.D. Tex. 2014), discussed Juhl, and held that "[e]ven if Texas

courts are open to recognizing aiding and abetting liability, it is

thus unlikely that they will extend it to claims for aiding and

abetting the competition-related torts at issue here." (citing W.

Fork Advisors, LLC v. SunGard Consulting Servs., LLC, 437 S.W.3d

917, 922 (Tex. App.–Dallas 2014, pet. filed). The court quoted

Hinojosa v. City of Terrel, Tex., 834 F.2d 1223, 1231 n. 12 (5th

Cir. 1988), which stated that "[a] party who wants a court to adopt

an innovative rule of state law should litigate in state rather

than federal court . . . Federal judges are disinclined to make

departures in areas of law that we have no responsibility for

23

developing."   (alterations in original)(citations omitted).

Thus, the court finds that there is no authority under Texas law for allowing an aiding and abetting liability theory to be applied to the competition- and theft-related torts asserted in this case. Plaintiffs argue that Defendants' behavior in this case was damaging to many victims because it was a theft of their personal information, and the court should therefore recognize aiding and abetting liability in this case. The court acknowledges that the deliberate theft of personal information is abhorrent, but under the particular facts of this case, cannot agree that it falls within the "dangerous or antisocial" category suggested by Juhl.

Therefore, Plaintiffs' aiding and abetting claims against Antonini related to misappropriation of confidential information, conversion, trespass to chattels, unfair competition, and tortious interference with business relationships must be dismissed.

D.   Civil Conspiracy

Antonini moves to dismiss Plaintiffs' civil conspiracy claims against him under the CFAA, SCA, TUTSA, THACA, and TTLA.

The elements of civil conspiracy are: (1) two or more persons; (2) an object to be accomplished; (3) a meeting of the minds on the object or course of action; (4) one or more unlawful, overt acts; and (5) damages as a proximate result. Tri v. J.T.T., 162 S.W.3d 552, 556 (Tex. 2005); Meineke Discount Muffler v. Jaynes, 999 F.2d 120, 124 (5th Cir. 1993).   "Civil conspiracy is a

derivative tort" under Texas law, so a plaintiff must "state a separate underlying claim on which the court may grant relief," or the conspiracy claim fails. Meadows v. Hartford Life Ins. Co., 492 F.3d 634, 640 (5th Cir. 2007).

1. Elements of Civil Conspiracy

Antonini generally challenges Plaintiffs' civil conspiracy against him, arguing that Defendants have not proven or provided evidence of any of the elements of a civil conspiracy. However, at this stage of the case, the court is looking not at whether Plaintiffs have provided evidence or proven their claims. Instead, the court looks to the allegations contained in the complaint and determines if claims have been adequately pled. In their complaint, Plaintiffs pled that all defendants conspired together to unlawfully appropriate their trade secrets and information which caused damage to Plaintiffs. Plaintiffs' factual allegations contain a number of overt acts, including the rounds of hacking by Defendants, in the furtherance of this conspiracy. After a review of the live pleading, the court finds that the complaint is not factually deficient.

2. Statute of Limitations

The statute of limitations for civil conspiracy in Texas is two years. See Doe v. St. Stephen's Episcopal Sch., No. C-08-299, 2008 WL 4861566, at *3 (S.D. Tex. Nov. 4, 2008)(unpublished)(citing Tex. Civ. Prac. & Rem. Code § 16.003 and cases). Under Texas law,

this "two-year limitations period governs conspiracy claims even if a longer statute-of-limitations period applies to the underlying tort." Agar Corp., Inc. v. Electro Circuits Int'l, LLC, No. 14-15-00134-CV, 2016 WL 7436811, at *4 (Tex. App.–Houston [14th Dist.] Dec. 22, 2016, no pet.)(unpublished).

Normally, when a claim accrues, the statute of limitations starts running. Id. at *5. However, under the continuing tort exception, "when wrongful conduct is repeated over time, each wrongful act can create a separate claim that does not accrue until the conduct ends." Id. (citing cases). "[C]are must be taken to distinguish between (1) repeated injury proximately caused by repetitive wrongful or [tortious]. . . acts and (2) continuing injury arising from one wrongful act. While the former evinces a continuing tort, the latter does not." Id. at *6 (citing Rogers v. Ardella Veigel Inter Vivos Trust No. 2, 162 S.W.3d 281, 290 (Tex. App.–Amarillo 2005, pet. denied)). "[U]nder civil conspiracy, each continued invasion of the plaintiff's interest causing loss and damage in a conspiracy case is treated as an independent element for limitations purposes and the two year statute of limitations begins to run when each independent element arises." Mayes v. Stewart, 11 S.W.3d 440, 453 (Tex. App.–Houston [1st Dist.] 2000, pet. denied)(quoting Cathey v. First City Bank, 758 S.W.2d 818, 822 (Tex. App.–Corpus Christi 1988, writ denied)).

Limitations is an affirmative defense. Noe v. LPP Mortg.

Ltd., No. H-11-3798, 2013 WL 12141260, at *4 (S.D. Tex. Mar. 29, 2013)(unpublished)(citing Abecassis v. Wyatt, 785 F. Supp.2d 614, 652 (S.D. Tex. 2011)). "[B]ecause the period of limitations is an affirmative defense it is rarely a good reason to dismiss under Rule 12(b)(6)." Noe, 2013 WL 12141260, at *4 (citing Abecassis, 785 F. Supp.2d at 652 (quoting Reiser v. Residential Funding Corp., 380 F.3d 1027, 1030 (7th Cir. 2004))). "A court should dismiss based on the statute of limitations only if that bar to relief appears on the face of the complaint or other appropriately considered materials." Noe, 2013 WL 12141260, at *4 (quoting Abecassis, 785 F. Supp.2d at 651 (citing Garrett v. Commonwealth Mortg. Corp. of Am., 938 F.2d 591, 594 (5th Cir. 1991))).

Responding to Antonini's arguments that the specific, underlying claims should be dismissed based on their applicable statutes of limitation, the court finds only the statute of limitations for civil conspiracy applies in this context. Plaintiffs allege that Defendants continued their wrongful conduct through January 2016, well within two years of the filing of the complaint. The multiple rounds of hacks allegedly caused repeated injury to Plaintiffs. Therefore, the court finds that Plaintiffs' civil conspiracy claims should not be dismissed based on limitations at this time.

3.   Federal Computer Access Violations

Plaintiffs allege that Antonini conspired to violate 18 U.S.C.

("Section") §§ 1030(a)(2)(C), 1030(a)(4), 1030(a)(5)(A), 1030(g), 2701(a)(1), and 2707.   Antonini challenges Plaintiffs' conspiracy claim, arguing that there is no common-law civil conspiracy claim under the CFAA and that the only way to bring a conspiracy claim to commit a CFAA violation is via the CFAA's conspiracy provision, Section 1030(b).   In a related argument, Antonini contends that there cannot be a civil conspiracy claim under the SCA.

Finally, Antonini argues that, because fraud is involved, Plaintiffs should have to meet the Rule 9(b) standard.

a.   Rule 9(b)

While fraud is involved in these statutory claims, violations of these statutes are distinguishable from common-law fraud which requires an actionable misrepresentation.   Antonini has cited no authority, and the court is aware of none, that the Fifth Circuit requires plaintiffs to meet the heightened pleading standard of Rule 9(b) for these computer access violations.   Therefore, the court finds Antonini's argument to be without merit.

b.   Common-Law Conspiracy to Violate the CFAA and SCA

The CFAA creates civil and criminal penalties for computer-related activities. See Fiber Sys. Int'l, Inc. v. Roehrs, 470 F.3d 1150, 1156 (5th Cir. 2006); 18 U.S.C. § 1030(a)(1)-(7).   Section 1030(b) imposes liability on a person who conspires to commit an offense under Section 1030.

Section 1030(g) enables a plaintiff to bring a civil action

for violations of the CFAA. Roehrs, 470 F.3d at 1156-57; 18 U.S.C. § 1030(g).   However, Section 1030(g)'s authorization of a civil suit is not coextensive with the entire statute.   The statute states in relevant part, "A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in subclauses (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(i)."   See 18 U.S.C. § 1030(g).

In Roehrs, the court reversed a lower court's determination that Section 1030(g)'s grant of civil liability was limited only to the predecessor section to Section 1030(c)(4)(A)(i), and found that Section 1030(g) extended civil liability to any person suffering a damage for a violation of Section 1030 as long as one of the five factors under subsection (a)(5)(B), now (c)(4)(A)(i), was present.

Antonini argues that the CFAA, by creating a statutory conspiracy claim, excludes common-law conspiracy claims. The court agrees.   Plaintiffs' ability to bring a civil conspiracy claim arising out of a violation of Section 1030 must be considered within the confines of that section.   Here, to the extent that Plaintiffs allege a conspiracy under the CFAA, the court will consider it a statutory conspiracy claim under Section 1030(b), and finds that Plaintiffs adequately pled this claim against Antonini.

The SCA makes it unlawful to intentionally access without authorization a facility through which an electronic communication service is provided. 18 U.S.C. § 2701(a)(1). Section 2707 allows a plaintiff to bring a civil action and recover damages for

violations of the SCA. 18 U.S.C. § 2707(a). Section 2708 states that "[t]he remedies and sanctions described in this chapter are the only judicial remedies and sanctions for nonconstitutional violations of this chapter." 18 U.S.C. § 2708. Notably, the SCA does not contain a conspiracy provision.

As the SCA states that the remedies provided are exclusive, the court will not imply a state law conspiracy remedy for violations of the SCA. Therefore, Plaintiffs' common-law conspiracy claims under the SCA and CFAA against Antonini must be dismissed.

c. Negligent Design

Antonini argues that to the extent that Plaintiffs' conspiracy to violate the CFAA claim hinges on damages from negligent design of computer software, it should be dismissed because this is not a valid claim under the CFAA.

The court agrees that actions for negligent design of software are not actionable under the CFAA. See 18 U.S.C. § 1030(g)("No action may be brought under this subsection for the negligent design or manufacture of computer hardware, computer software, or firmware."). However, Plaintiffs have not alleged that Antonini conspired to violate the CFAA through negligent design of software. Therefore, there is no cause of action based on negligent design of software to dismiss.

d. Statute of Limitations

Antonini argues that any conspiracy claim under the CFAA or SCA is barred by limitations. As the court has recommended that Plaintiffs' common-law conspiracy claims under the CFAA and SCA be dismissed, the court will only consider whether the statute of limitations bars a statutory conspiracy claim under the CFAA.

18 U.S.C. § 1030(g) establishes a two-year statute of limitations for claims under the CFAA, subject to the discovery rule. 18 U.S.C. § 1030(g)("No action may be brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the date of the discovery of the damage."). Under federal law, "[a] cause of action accrues at the time the plaintiff knows or has reason to know of the injury which is the basis of the complaint. In the conspiracy context, the cause of action accrues as soon as the plaintiff knew or should have known of the overt acts involved in the alleged conspiracy." Shabazz v. Franklin, 24 F.3d 239, 1994 WL 243356, at *1 (5th Cir. 1994)(unpublished)(citing Helton v. Clements, 832 F.2d 332, 334-35 (5th Cir. 1987)).

Plaintiffs have alleged unlawful activities by Defendants from October 2013 through 2016, and they filed their complaint in June 2016. It is unclear on the face of the complaint, especially with the addition of the discovery rule, which actions may be barred under the statute of limitations. Therefore, the court declines to dismiss on this basis.

4.   TUTSA and TTLA

Antonini argues that Plaintiffs' claim of conspiracy to violate the TUTSA should be dismissed because: (1) Defendants' conduct is reverse engineering; (2) actions prior to the inception of the TUTSA are not actionable; and (3) the complaint does not contain facts to support a claim against Antonini.

The TUTSA provides for injunctive relief and/or damages for misappropriation of trade secrets. Tex. Civ. Prac. & Rem. Code §§ 134A.001–.004. "Trade secret misappropriation under Texas law is established by showing: (a) a trade secret existed; (b) the trade secret was acquired through a breach of a confidential relationship or discovered by improper means; and (c) use of the trade secret without authorization from the plaintiff." Spear Mktg., Inc. v. Bancorpsouth Bank, 791 F.3d 586, 600 (5th Cir. 2015)(citations omitted). A TUTSA claim "requires that a defendant 'acquire' knowledge of the trade secret at issue through 'improper means.'" Capstone Associated Servs., Ltd. v. Organizational Strategies, Inc., No. H-15-3233, 2015 WL 9319239, at *2 (S.D. Tex. Dec. 23, 2015)(unpublished)(internal quotes in original)(citing Educ. Mgmt. Servs., LLC v. Tracey, 102 F. Supp.2d 906, 914 (W.D. Tex. 2015)(internal citations omitted)).

a.   Reverse Engineering

Under the TUTSA, "'reverse engineering' means the process of studying, analyzing, or disassembling a product or device to

32

discover its design, structure, construction, or source code provided that the product or device was acquired lawfully or from a person having the legal right to convey it." Tex. Civ. Prac. & Rem. Code § 134A.002(5). "'Proper means' means discovery by independent development, reverse engineering unless prohibited, or any other means that is not improper." Tex. Civ. Prac. & Rem. Code § 134.002(4).

The court finds that the TUTSA claim should not be dismissed based on the "reverse engineering" exclusion. It is unclear how Defendants' actions in this case constitute "reverse engineering" under the TUTSA and Antonini provides no explanation to show how the trade secrets alleged by Plaintiffs were acquired lawfully by Defendants in this case.

b. Facts Supporting the Claim

Plaintiffs have pled that their trade secrets, which consist of their member information and Google Analytics data, were misappropriated by Defendants through the series of unauthorized hacks that Antonini, as chief of technology of Oilpro, conspired in. Plaintiffs allege that Antonini, along with David Kent, was most familiar with Rigzone's code. The court finds that this is enough to survive a motion to dismiss Plaintiffs' conspiracy to violate the TUTSA claim.

c. Preemption of the TTLA

Antonini seeks to dismiss Plaintiffs' claims that he conspired

33

to violate the TTLA, arguing that it is preempted by the TUTSA.

Plaintiffs argue that this claim is not based on the theft of trade

secrets, but instead on the wrongful access and resulting harm to

Plaintiff's confidential information and property, and therefore it

is not preempted by the TUTSA.

Before the inception of the TUTSA, the TTLA provided a civil

remedy for the misappropriation of trade secrets under Texas law.

In re Mandel, 578 F. App'x 376, 384 n. 8 (5th Cir.

2014)(unpublished). The TUTSA states that "this chapter displaces

conflicting tort, restitutionary, and other law of this state

providing civil remedies for misappropriation of a trade secret."

Tex. Civ. Prac. & Rem. Code § 134A.007(a). This section of the

TUTSA took effect on September 1, 2013, and superceded the civil

remedy under the TTLA for misappropriation of trade secrets "made

on or after" its effective date. Mandel, 578 F. App'x at 384 n. 8.

Therefore, to the extent that Plaintiffs bring a misappropriation

of trade secrets claim related to activity prior to the TUTSA's

effective date, it is only actionable under the TTLA, not the

TUTSA.

In Plaintiffs' complaint, Plaintiffs allege that the TTLA was

violated by Defendants when they "knowingly and unlawfully

appropriated Plaintiffs' property with the intent to deprive

Plaintiffs of their exclusive use of their member information and

their Google Analytics data."[105]   However, later in Plaintiffs'
complaint, they allege that their "proprietary member information,
internet search methods, and Google Analytics data constitute trade
secrets within the meaning of the Texas Uniform Trade Secrets
Act."[106]   While Plaintiffs are alleging in their TTLA claim that
Defendants' appropriation of their property deprived them of
exclusive use of their member information and Google Analytics
data, it is unclear to what "property" they could be referring in
this context, other than the member information and Google
Analytics data.   Therefore, because their TTLA claim is based on
the misappropriation of trade secrets, the TTLA is preempted in
this context by the TUTSA for any claims on or after September 1,
2013. In Plaintiffs' complaint, they allege that Defendants' began
hacking their systems in October 2013, after the TTLA was
preempted.   Therefore, Plaintiffs' claims under the TTLA must be
dismissed.

   5.   THACA

   Antonini moves for dismissal of Plaintiffs' claim that he
conspired to violate the THACA, also arguing that this claim is
preempted by the TUTSA.

   Under Texas Civil Practice and Remedies Code § 143.001, "[a]
person who is injured or whose property has been injured as a

---

[105]   See Doc. 1, Pls.' Compl. pp. 43-44.

[106]   See id. p. 38.

result of a violation under Chapter 33, Penal Code, has a civil cause of action if the conduct constituting the violation was committed knowingly or intentionally." Tex. Civ. Prac. & Rem. Code § 143.001. Texas Penal Code § 33.02 provides: "A person commits an offense if the person knowingly accesses a computer, computer network, or computer system without the effective consent of the owner." Tex. Penal Code. § 33.02(a).

In Plaintiffs' complaint, Plaintiffs allege that Defendants violated the THACA because they "knowingly and intentionally accessed a computer, computer network, or computer system without the effective consent of the owners."[107] Here, the court finds that this claim is not based on misappropriation of a trade secret; rather, it is based on Defendants' wrongful access of Plaintiffs' computer systems and networks. Therefore, Antonini's motion to dismiss must be denied on this basis.

IV.   Conclusion

Based on the foregoing, the court **RECOMMENDS** that Antonini's motion to dismiss be **GRANTED IN PART** and **DENIED IN PART.** The court **RECOMMENDS** that the following claims be **DISMISSED:** Plaintiffs' claims of aiding and abetting the following state law causes of action: misappropriation of confidential information, conversion, trespass to chattels, unfair competition, and tortious interference with business relationships; Plaintiffs' common-law conspiracy

---

[107]   See Doc. 1, Pls.' Compl. p. 42.

claims under the CFAA and SCA; and Plaintiffs' claim of conspiracy to violate the TTLA.

The Clerk shall send copies of this Memorandum and Recommendation to the respective parties who have fourteen days from the receipt thereof to file written objections thereto pursuant to Federal Rule of Civil Procedure 72(b) and General Order 2002-13. Failure to file written objections within the time period mentioned shall bar an aggrieved party from attacking the factual findings and legal conclusions on appeal.

The original of any written objections shall be filed with the United States District Clerk electronically. Copies of such objections shall be mailed to opposing parties and to the chambers of the undersigned, 515 Rusk, Suite 7019, Houston, Texas 77002.

SIGNED in Houston, Texas, this 27<u>th</u> day of April, 2017.

_____
U.S. MAGISTRATE JUDGE